3GPP TSG SA WG3 Security — S3#32
Edinburgh, UK, 9-13 February 2004

Tdoc ⌘S3-040074

CR-Form-v7

Pseudo CHANGE REQUEST

⌘ **33.221** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Further clarifications on certificate profiles and certificate request
Source:	⌘	Nokia
Work item code:	⌘	GAA
Date:	⌘	30/1/2004
Category:	⌘	
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	Further clarifications were needed on the usage of certain profiles.
Summary of change:	⌘	Current TS has an editor's note that the applicability of certificate profiles such as qualified certificate profiles defined by ETSI, and attribute certificate profile defined by IETF should be studied further. There are two **qualified certificate profiles** defined by IETF (RFC 3039) and by ETSI (ETSI TS 101 862). In order to call a certificate *qualified* both the end entity and the CA must follow much stricter requirements on where the private key is stored, how the certificate enrollment is protected, and how the certificate is used. Generic requirement on *certification practices* have been defined in EU Directive on electronic signatures. If operator follows these requirements then the issued subscriber certificates can also be called qualified certificates. **Attribute certificate profile** (RFC 3281) is not applicable to subscriber certificates because subscriber certificates are based on *public key certificates*, where an indentity is tied to a public key. Attribute certificate is used to tie an identity to a set of attributes. Hence, the attribute certificate profile is out side the scope of the SSC TS. Also other certificate profiles that are based on X.509 certificate profile can be used but it is recommended to use the WAP certificate and CRL profile for subscriber certificates. **Clarification on certificate request:** the certificate request should not be mandated to contain any of the attributes listed in section 4.2.6.
Consequences if	⌘	

not approved:	

Clauses affected:	⌘	4.2.6			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******* END CHANGE *******

2 References

...

[15] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[16] Santesson, S., Polk, W., Barzin, P., and M. Nystrom, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", RFC 3039, January 2001.

[17] ETSI TS 101 862: "Qualified certificate profile".

******* BEGIN CHANGE *******

4.2.6 Subscriber Certificate Profile

Subscriber certificate profile shall be based on WAP Certificate and CRL Profile [7], which in turn is based on profiles defined in [6] and [10]. A certificate profile defines the format and semantics of certificates in a specific context. WAP Certificate and CRL profiles specification defines four certificate profiles: two user certificate profiles – one for authentication and the other for non-repudiation purposes, server certificate profile for authentication, and authorization certificate profile (i.e., CA certificate). Since subscriber certificates are issued to users, and since services need CA certificate to validate subscriber certificates, the relevant WAP certificate profiles to be used with subscriber certificate profiles are the user certificate profiles, and CA certificate profile.

~~Editor's note: Applicability of other certificate profile specifications, e.g. RFC 3281, ETSI QC profile is FFS.~~

IETF's and ETSI's Qualified certificate profiles [16,17] may also be used as the subscriber certificate profile if the certification practices followed by the certificate issuing operator fulfil all of the requirements stated in [15,16,17].

The following certificate extensions ~~shall~~may be filled with the information given by the UE in the certification request:

- Intended certificate usage (i.e., using keyUsage and/or extKeyUsage extensions [7]).
- Subscriber identities (i.e., subject name field, and possible additional identities defined in the subjectAltName extension [7]). Operator CA shall authorize each suggested subscriber identity.
- Proof of key origin (i.e., keyGenAssertion). Operator CA shall verify the proof of key origin if it is presented.

NOTE: It is not mandatory for Operator CA to insert these suggested extensions by UE to the certificate. Rather, Operator CA shall issue certificates based on its certification policies. It may write a certification practice statement (CPS) [4], where it describes the general requirements and steps taken during the certificate issuing.

******* END CHANGE *******